Project 5: Disaster recovery with IBM cloud virtual server

Name : Poojasree

Register no : 411521104082

Project Title: Disaster Recovery

Problem Statement:

The world of disaster recovery with IBM cloud virtual server .Disaster recovery, which also includes cloud-based DR, is part of a broader BC umbrella. It typically plays a central role in many avenues of BC planning, such as for floods, earthquakes and cyber-attacks.

For example, if the business operates on a known earthquake fault, the risk of damage from an earthquake would pose a potential risk that would be analysed to formulate a mitigation plan. Part of the mitigation plan might be to adopt cloud DR in the form of a second hot site located in a region free of earthquake danger.

Thus, the BC plan would rely on redundancy of the cloud DR service to seamlessly continue operations in the event that the primary data centre became unavailable, continuing business operations. In this example, DR would only be a small part of the BC plan, with additional planning detailing corresponding changes in workflows and job responsibilities to maintain normal operations -- such as taking orders, shipping products and handling billing -- and work to restore the affected resources.

Phase 1: Problem Definition and Design Thinking:

Problem Definition:

Building a cloud DR plan is virtually identical to more traditional local or off-site disaster recovery plan. The principal difference between cloud DR and more traditional DR approaches is the use of cloud technologies and DRaaS to support an appropriate implementation. For example, rather than backing up an important data set to a different disk in another local server, cloud-based DR would back up the data set to a cloud resource such as an amazon simple service bucket. As another example, instead of running an important server as a warm VM in a colocation facility, the warm VM could be run in Microsoft Azure or through any number of different DRaaS providers. Thus, cloud DR doesn't change the basic need or steps to implement DR, but rather provides a new set of convenient tools and platforms for DR targets.There are three fundamental components of a cloud-based disaster recovery plan: analysis, implementation and testing.

Design Thinking:

Design thinking is a human-centred approach to problem- solving and project design that focuses on understanding user needs, ideating creative solutions, and iteratively refining those solutions. When applied to a project like "disaster recovery with IBM cloud virtual server," it can help ensure that the final solution meets the needs to be able to recover quickly from any event that stops day by day operation. Here's a design thinking approach for such a project:

1. ***Empathize:*** *Following disaster, people frequently feel stunned, disoriented or unable to integrate distressing information.*

Once these initial reactions subside, people can experience a variety of thoughts and behaviours.

Research shows that most people are resilient and over time are able to bounce back from tragedy. It is common for people to experience stress in the immediate aftermath, but within a few months most people are able to resume functioning as they did prior to the disaster. It is important to remember that resilience and recovery are the norm, not prolonged distress.

2. ***Define:*** *Clearly Define the Problem and Goals*

Disaster recovery (DR) is an organization's ability to restore access and functionality to IT infrastructure after a disaster event, whether natural or caused by human action (or error).

3. ***Ideate:*** *A disaster recovery plan (DR or DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events.*

4. ***Prototype:*** *Develop a Proof of Concept*

The prototype planning tool helps address this need, but requires further work to validate and test the inputs and functions already included, especially the functions used to calculate disaster effects.

Use of the prototype tool would enable systematic testing of the data and estimates used in the planning tool to inform its further development. Similarly, feedback from potential users, including government agencies, on ways that both sets of tools may be improved would support future efforts to refine them

5. ***Test:*** *Disaster recovery testing is the process to ensure that an organization can restore data and applications and continue operations after an interruption of its services, critical IT failure or complete disruption. It is necessary to document this process and review*

it from time to time with their clients. It will ensure that you know how to save your client in the event of any fail. Keep reading to learn more about disaster recovery testing scenarios and disaster recovery testing best practices.

6. ***Implement:*** *Build the Full-Scale Solution:*

Once the prototype is refined and validated, proceed to develop the full-scale solution for disaster recovery with IBM cloud virtual servers

Collaborate with the IT team to ensure that the infrastructure is properly set up and configured for scalability and performance.

7. ***Monitor and Learn:*** *Continuously Improve:*

Monitoring is the regular collection of information about all project activities. It shows whether things are going according to plan and helps project managers to identify and solve problems and or issues identified in a prompt manner.

The learning we obtain from these evaluations is incorporated into program design and delivery.

Therefore, disaster recovery is a set of activities deployed to achieve the desired recovery objective and outcome after the occurrence of a disaster.

8. ***Deliver and Scale:*** *Deploy the Solution:*

Deploy the final solution for disaster recovery with IBM cloud virtual servers to production.

Scale the system as needed to minimise the impacts of an unexpected incident.

Provide training and support to users and organization.

9. ***Evaluate Impact:*** *Measure Business Outcomes:*

Evaluate the impact of the disaster recovery solution on the organization's goals and objectives.

Measure improvements in customer retention; reduce recovery cost, or other relevant metrics.

Adjust the solution and strategies as needed based on the evaluation results.

10. ***Iterate and Innovate:*** *Continue Refining:*

Design thinking is an iterative process. Continue to gather feedback, iterate on the solution, and innovate to address evolving user needs and business requirements.

Stay informed about advancements in disaster recovery technologies and consider their potential application.

Disaster Recovery:

Disaster recovery (CDR) is simple to configure and maintain, as opposed to conventional alternatives. Companies no longer ought to waste a lot of time transmitting data backups from their in-house databases or hard drive to restore after a tragedy. Cloud optimizes these procedures, decisions correctly, and information retrieval.

Disaster recovery planning guide:

- Disaster recovery building blocks
- Disaster recovery scenarios for data
- Disaster recovery scenarios for applications (this article)
- Architecting disaster recovery for locality-restricted workloads
- Disaster recovery use cases: locality-restricted data analytic applications

Understand Your Backup Needs:

The first step to creating an effective disaster recovery system is to understand:

- What information needs to be backed up
- Why that information needs to be backed up
- How that information will be backed up

Document Disaster Recovery Activities:

Disaster recovery requires documentation. Keep a playbook that defines the disaster recovery activities that need to occur each day, week, month, and year. Determine what needs to be saved and why. Also determine what is no longer necessary to keep, like past customer or employee information. Consider compliance while reviewing this documentation.

Disaster Recovery Strategy:

Cloud disaster recovery, often called cloud DR, is a comprehensive approach encompassing strategies and services for safeguarding data, applications, and assets by replicating them to public cloud environments or dedicated service providers. In a disaster, this replicated data can be used to restore affected systems to a local data center or a cloud provider, enabling the enterprise to resume its standard operations. The core objective of cloud DR mirrors that of traditional cloud disaster recovery strategy: to protect critical business resources and guarantee their accessibility and recoverability, thereby ensuring uninterrupted business continuity.

Picking a Cloud Disaster Recovery Provider:

When choosing a cloud disaster recovery (DR) provider, a company should take into account the following five key factors:

1) Scalability:

Evaluate the scalability of the cloud DR solution, ensuring it can safeguard designated data, applications, and assets. It should also have the capability to expand to accommodate additional resources, delivering consistent performance even as other clients globally utilize the services.

2) Security and Compliance:

Comprehend the security prerequisites for your DR content and confirm that the provider can provide essential security measures like authentication, virtual private networks, encryption, and other tools required to protect your valuable assets. Assess compliance demands to guarantee that the provider holds certifications aligning with business- related compliance standards, like Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, SOC 2, and SOC 3.

3) Reliability:

Assess the dependability of the cloud DR provider. While even cloud services may encounter downtime, it’s crucial to avoid service interruptions during recovery, as they can harm the business equally.

4) Distance:

A business should consider the physical proximity and latency of the cloud DR provider. Placing DR too nearby increases the vulnerability to shared physical disasters while locating it too far can lead to latency and network congestion, hampering DR content accessibility. The situation becomes more complex when the

DR content is required to be accessible from numerous global business sites.

5) Architecture:

Examine the architectural requirements of the DR platform. DR can be approached through three fundamental methods: cold, warm, and hot disaster recovery. These terms roughly correspond to the simplicity of system recovery.

A Cloud Disaster Recovery service offers organizations several benefits, including:

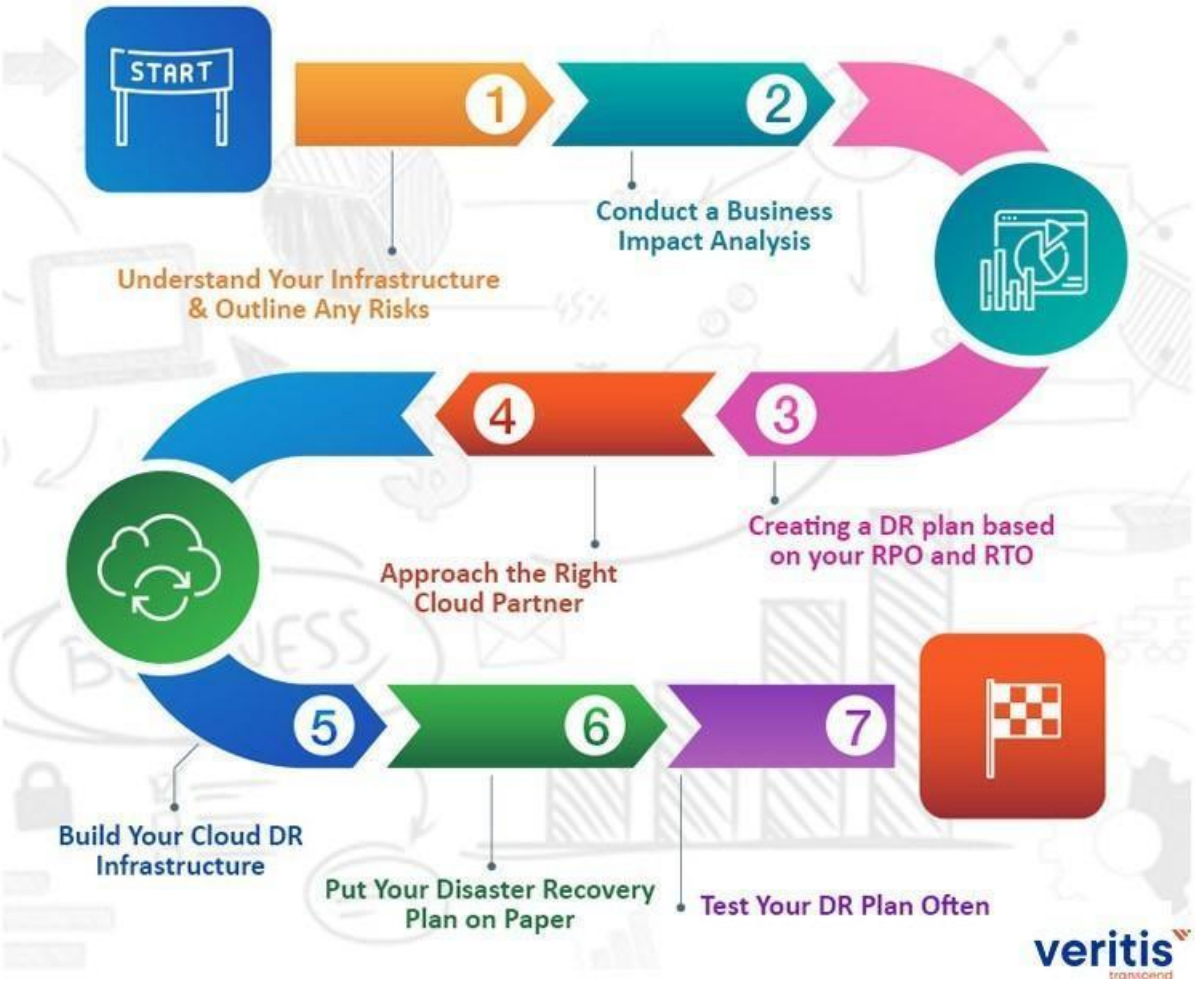
- Saves Time/Capital
- More Data Backup Location Options
- Easy to Implement with High Reliability
- Scalability

For considering cloud disaster recovery for the first time and are wondering where to start, here's an easy cloud disaster recovery plan that will help you plan and effective disaster recovery service. It is inevitable for organizations to have a disaster recovery (DR) strategy to protect their Vault deployment against catastrophic failure of an entire cluster. Vault Enterprise supports multi-data center deployment where you can replicate date across data centers for performance as well as disaster recovery.

A cluster is the basic unit of Vault Enterprise replication which follows the leader-follower model. A leader cluster is referred to as the primary cluster and is considered the system of record. Data is streamed from the primary cluster to all secondary (follower) clusters. Primary clusters can stream data to both disaster recovery secondary clusters and performance replication.

In this tutorial you will setup disaster recovery replication and simulate a failure to the primary cluster.

Cloud Disaster Recovery Plan



•